Amendment to the Claims:

Claim 1 (Currently Amended): A method for re-learning a previously programmed key within an electronic control module of a security system, comprising:

transmitting a key identification code from the previously programmed key to the electronic control module;

executing an authentication protocol for the previously programmed key; [[and]]

said authentication protocol comprising the step of comparing said key identification code to a disabled identification code;

~~storing~~ restoring said key identification code [[in]] to an active status within the electronic control module when said key identification code is identical to said disabled identification code.

Claim 2 (Original): The method as recited in claim 1 wherein executing said authentication protocol comprises:

comparing said key identification code to at least one disabled identification code that is stored within the electronic control module.

Claim 3 (Original): The method as recited in claim 2 wherein executing said authentication protocol comprises:

determining that said key identification code is identical to at least one disabled identification code stored within the electronic control module.

Claim 4 (Original): The method as recited in claim 1 wherein executing said authentication protocol comprises:

determining that the previously programmed key and the electronic control module share a common unique secret code, said common unique secret code utilized with an encryption algorithm for encrypting a signal and allowing encrypted communication between the previously programmed key and the electronic control module.

Claim 5 (Currently Amended): The method as recited in claim 4 [[1]] wherein executing said authentication protocol comprises:

transmitting at least one of said key identification code and said common unique secret code from a supplementary database to the electronic control module.

Claim 6 (Currently Amended): A method for re-learning a key within an electronic control module, comprising:

transmitting a key identification code from the previously programmed key to the electronic control module;

executing an authentication protocol for the previously programmed key; and

said authentication protocol comprising the step of comparing said key identification code to a disabled identification code;

~~storing~~ restoring at least one of a key password and said key identification code [[in]] to an active status within the electronic control module when said key identification code is identical to said disabled identification code.[[;]]

~~wherein executing said authentication protocol includes transmitting a valid response signal from the previously programmed key to the electronic control module, said valid response signal including said key password.~~

Claim 7 (Original): The method as recited in claim 6 wherein executing said authentication protocol comprises:

determining that the previously programmed key and the electronic control module share a common unique secret code, said common unique secret code utilized with an encryption algorithm for encrypting a signal and allowing encrypted communication between the previously programmed key and the electronic control module.

Claim 8 (Original): The method as recited in claim 7 wherein determining that the previously programmed key and the electronic control module share a common unique secret code, comprises:

encrypting a signal with said common unique secret code, said signal having a predetermined data;

transmitting said signal from the electronic control module to the previously programmed key; and

comparing said predetermined data to a key authentication data stored within the previously programmed key.

Claim 9 (Original): The method as recited in claim 8 wherein transmitting said valid response signal from the previously programmed key to the electronic control module comprises:

determining that said predetermined data is identical to said key authentication data.

Claim 10 (Original): The method as recited in claim 8 wherein executing said authentication protocol comprises:

comparing said key password to at least one module password stored within the electronic control module.

Claim 11 (Original): The method as recited in claim 10 further comprising:

determining that said key password is identical to said at least one module password.

Claim 12 (Original): The method as recited in claim 6 wherein executing said authentication protocol comprises:

comparing said key identification code to at least one disabled identification code that is stored within the electronic control module.

Claim 13 (Original): The method as recited in claim 12 further comprising:

determining that said key identification code is identical to said at least one disabled identification code.

Claim 14 (Original): The method as recited in claim 6 wherein executing said authentication protocol comprises:

transmitting at least one of said key identification code, a unique secret code, and a module password from a supplementary database to the electronic control module.

Claim 15 (Original): The method as recited in claim 14 further comprising at least one of:

comparing said key identification code to at least one disabled identification code stored in the electronic control module; and

comparing said key password to said module password.

Claims 16-17 (Cancelled)

Claim 18 (Currently Amended): The security system of claim 21 [[16]] wherein said microprocessor includes an encryption algorithm for encrypting a signal with said unique secret code, said microprocessor including control logic for storing said key identification code when said key transmits a valid response signal to said primary electronic control module.

Claim 19 (Currently Amended): The security system of claim 21 [[16]] wherein said microprocessor includes an encryption algorithm for encrypting a signal with said unique secret code, said microprocessor including control logic for storing said key identification code when said key transmits a key password that is identical to said module password.

Claim 20 (Cancelled)

Claim 21 (New): A security system for re-learning a key into an electronic control module, comprising:

a primary electronic control module comprised of an antenna, a memory, and a microprocessor coupled to said antenna and said memory; and

a previously programmed key having electronic circuitry with a key identification code stored therein, said previously programmed key further including a transponder for transmitting said key identification code to said antenna of said primary electronic control module;

said antenna transmitting said key identification code to said microprocessor;

said memory having at least one of a disabled identification code, a unique secret code, and a module password stored therein;

said microprocessor executing an authentication protocol for the previously programmed key, said authentication protocol including comparing said key identification code to said disabled identification code;

said microprocessor including control logic for restoring said disabled identification code to an active status when said microprocessor determines that said key identification code is identical to said disabled identification code.

Claim 22 (New): A security system for re-learning a key into an electronic control module, comprising:

a primary electronic control module comprised of an antenna, a memory, and a microprocessor coupled to said antenna and said memory;

a previously programmed key having electronic circuitry with a key identification code stored therein, said previously programmed key further including a transponder for transmitting said key identification code to said antenna of said primary electronic control module;

said antenna transmitting said key identification code to said microprocessor;

said memory having at least one of a disabled identification code, a unique secret code, and a module password stored therein;

said microprocessor executing an authentication protocol for the previously programmed key, said authentication protocol including comparing said key identification code to said disabled identification code; and

at least one of a supplementary electronic control module and an external database;

said supplementary electronic control module coupled to said primary electronic control module and intended to facilitate execution of said authentication protocol, said supplementary electronic control module for transmitting at least one of said key identification code, said unique secret code, and a key password to said primary electronic control module; and

said external database selectively coupled to said primary electronic control module and intended to facilitate execution of said authentication protocol, said external database for transmitting at least one of said key identification code, said unique secret code, and said key password to said primary electronic control module.

Claim 23 (New): The security system of claim 22 wherein said microprocessor includes an encryption algorithm for encrypting a signal with said unique secret code, said microprocessor including control logic for storing said key identification code when said key transmits a valid response signal to said primary electronic control module.

Claim 24 (New): The security system of claim 22 wherein said microprocessor includes an encryption algorithm for encrypting a signal with said unique secret code, said microprocessor including control logic for storing said key identification code when said key transmits a key password that is identical to said module password.